取扱説明書

Blind2 Ver2.77

ファイルの暗号化／復号化ソフト

※ 説明中の絵図でソフトのバージョンが 2.50 になっていますが画面デザイン
に変更ないのでそのまま使っています。悪しからずご了承ください。

- 使用する状況と目的 1
- Blind2の機能 1
- 操作画面の説明 2
- 暗号化／復号化の基本操作と手順 4
- 「簡単キー」について 7
- 使用条件 11

使用する状況と目的

パソコンを操作できる人が一家の中に何人かいると、一台のパソコンを家族で使う機会も多くなります。そうなると家族といえども、この書類は見られるのはちょっといやだなということもあります。

たとえば、年頃の娘さんの場合、パソコンで日記を書きたいけど留守の間に親から見られるのはいやだ。お父さんの場合、仕事でメールを使っているが仕事上家族にも見せられないものもある。お母さんの場合、パソコンで家計簿をつけているが、娘の友達が遊びに来ているときに間違って開かれるといやだ。などなど。一台のパソコンを複数の人たちで使っているとちょっと見られたくないというファイルがでてきます。

また、昨今はインターネットの常時接続を使用しているひとも増えて、インターネット上に仮想ディスクを用意し個人や法人に貸し出すビジネスも出てきました。インターネット上の仮想ディスクにファイルを預ける(コピーする)ときもやはり他人に見られるようで気持ち悪いし、その恐れもあります。こんなときも、簡単に暗号化できれば幾分は安心して預けられます。

Blind2はこのような時、簡単にファイルを暗号化できるソフトです。また、暗号化したファイルを元へ戻すことを複合化といい、複合化も基本的に暗号化と同じ操作で簡単にできます。

Blind2の機能

1. 一般ファイルの暗号化と復号化を行います。フォルダに対しては行えません。
   エクスプローラなどで対象となるファイル(暗号化したいファイル)を指定の場所にドラック・アンド・ドロップして、開始ボタンを押すと暗号化します。またこのとき対象となるファイルがすでに暗号化されたファイルであったら復号化を行います。
   ［注意］ 複数ファイルをまとめて暗号化／復号化する機能がいまのところありません。複数ファイルの

場合は圧縮ツールなどで1つのファイルにパッケージして暗号化してください。．．．いずれできるようにしたいと思っています。

2. 暗号化する場合パスワードを付けるモードと、あえて付けないモードがあります。
パスワードをつけなければ暗号化ではないという意見ももっともですが、家族の間で使う場合そこまでしなくてもよいという意見もありました。モラルとして見てはいけないファイルは自ずから見ない。ただうっかりダブルクリックなどをやって開く場合もあるので、これくらいを防止すればよいとの意見もまた納得できますのでこのモードをつけました。暗号化しているのは「見ないでね!」と意思表示しているファイルだということです。

3. パスワード忘却のために「簡単キー」を用意しました。
「パスワードは忘れるもの。」と、いうことで使用しているパスワードをフロッピーに書き込んで、フロッピーを差し込むことでパスワード入力を省く手段を用意しました。このフロッピーに書き込んだパスワードのことを「簡単キー」と名付けています。「簡単キー」は暗号化、復号化双方に使用できます。
これで暗号化したときのパスワードを忘れたとか、暗号化するときにパスワードを打ち間違いこれを気づかないままでいて、いざ復号化するときに、できないという事故が防げます。
「簡単キー」はフロッピーに作成されますので、フロッピーを抜きとり個人的に保管すれば他人が使うことはできません。．．．くれぐれも紛失しないように注意が必要です。
もちろん「簡単キー」そのものも暗号化され、他人は（自分も）見ることはできません。さらに「簡単キー」は単なるファイルですがこれを単純にコピーしても使用できないように施されています。．．．別のフロッピーにコピーしても使えません。

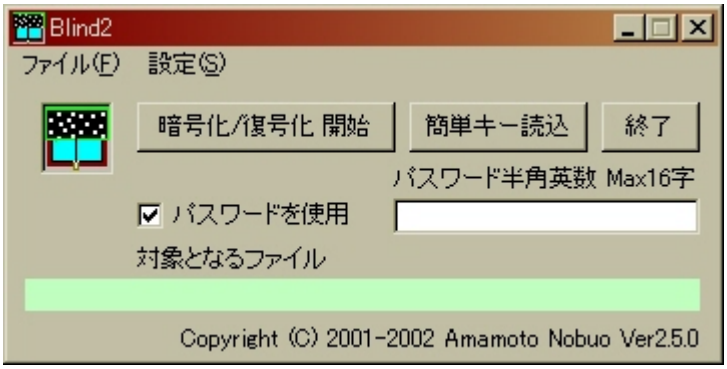
4. パスワードの間違いが多すぎるとストおこします。
暗号化したファイルを複合化するとき、パスワードをある回数続けて間違うとそれ以降は正しいパスワードが入力されても「パスワードが違っている」という旨のメッセージを表示し複合化をしないようにしています。これを解除するにはプログラムを再起動する必要があります。この最大間違い回数の数はセキュリティ上公開していません。

5. 「解除ファイル」というものもあります。
「簡単キー」の兄貴分に「解除ファイル」というものがあります。目的は「簡単キー」と同じですが「簡単キー」に比べ多少高機能になっています。例えば「簡単キー」は1つのパスワードしか保存できませんが「解除ファイル」は複数のパスワードを保存できます。また、賞味期限としてパスワードが有効な期限を切ることができます。
ただし、「解除ファイル」の作成は別プログラムで行います。Blind2では作成できません。この機能は作者自身が個人的に使用しているのみです。「解除ファイル」の作成プログラムはセキュリティの問題で現在公開していません。公開することにより暗号化されたファイルの解読にヒントが与えられる可能性があるため今のところその予定はありません。

操作画面の説明

1. 起動と起動画面

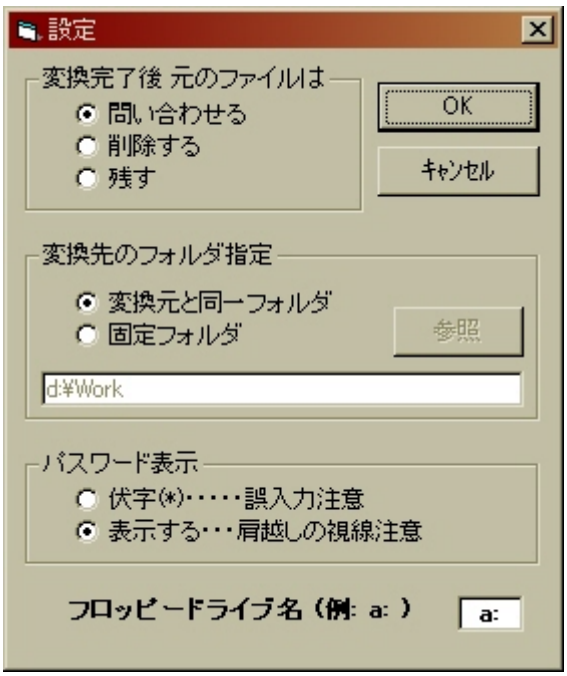
通常、Blind2を起動すると以下のような画面が表示されます。



最初に起動したときはまず設定画面を開き、自分に適した設定にするか、現状の設定状態を確認してください。
設定画面を開くには、メニューバーの「設定」－「設定画面」をクリックします。

2. 設定画面

設定画面は以下のようになっています。



各項目の説明をします。
「変換完了後　元のファイルは」の欄は、暗号化もしくは複合化をいた後、元になったファイルをどうするかの指定です。通常結果のファイルが正常に作成されていれば元になったファイルは消しても再現できるはずです。したがって消してもよいのですが心配な場合や他に理由があり残す場合もあるでしょう。
「問い合わせる」にチェックをいれるとその暗号化／復号化が完了する都度、元ファイルを消してもよいかを聞いてきます。「はい」で削除し、「いいえ」で残します。
「削除する」は暗号化／復号化が完了すると無条件に元ファイルは削除します。同様に「残す」は元ファイルは削除せずにそのまま残します。

使い慣れないときは「残す」もしくは「問い合わせる」にしておくのがよいかと思います。

「変換先のフォルダ指定」は暗号化／複合化の結果のファイルをどのフォルダに作成するかの指定です。「変換元と同一フォルダ」にチェックをいれると元ファイルのある同一フォルダに結果のファイルを作成します。
「固定フォルダ」にチェックをいれると変換ファイルは指定された固定フォルダに作られます。元ファイルがCD-ROM などにあり同一フォルダには結果ファイルの書き込みができない場合などに使用します。
また「固定フォルダ」にチェックを入れると右側にある参照ボタンが有効になりますのでこれを使うと固定フォルダ名の入力ミスが防げます。固定フォルダ名の入力にはできるだけ参照ボタン使うようにしてください。
ハードディスクにあるファイルを暗号化／復号化する場合は「変換元と同一フォルダ」にチェックをいれておくのがわかりやすいと思います。

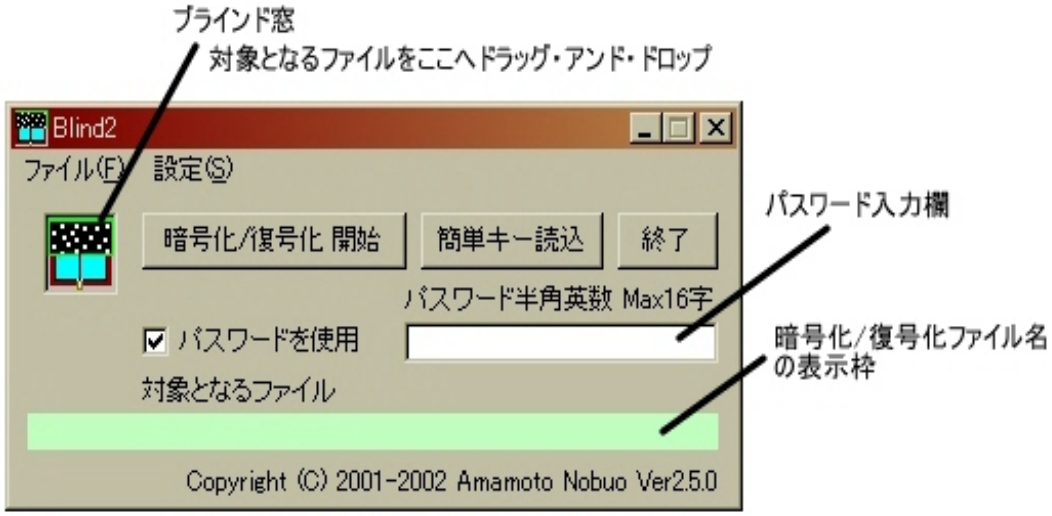
「パスワード表示」ついて。一般的にパスワードを入力するときはその入力欄には入力した文字列を表示させることはしません。通常 ＊ などの代替文字を表示し、肩越しからの傍観者に備えます。
会社などで人が集まるところでパスワードを打ち込む場合はこのような処置も必要かもしれませんが個人の家庭で一人で使用している場合はこのような処置はパスワードの誤入力を誘発するだけの余計な処置だと思います。それで設定で切り替えができるようにしました。
「伏字」にすると一般的な入力と同じように＊を代替文字とします。このときは誤入力に注意してください。「表示する」は通常のパスワードでない文字入力と同じように入力した文字列をそのまま表示します。自宅などで一人で使用している場合はこれでよいと思います。

「フロッピードライブ名」は現在はほとんどが a: のはずなので変更する必要はないと思います。NECの古いタイプを使っている人向けです。
この設定は「簡単キー」の作成のときと読込みのとき参照します。

暗号化／復号化の基本操作と手順

最初に言葉の定義をしておきます。あるファイルに暗号化を施し、新たにできたファイルをここでは「ブラインドファイル」と表現します。また、そのブラインドファイルの元になったファイルを「オリジナルファイル」と表現します。
すなわち、Blind2の目的はオリジナルファイルを暗号化してブラインドファイルを作成し、逆にブラインドファイルを復号化して元のオリジナルファイルを復元するものといえます。

1. オリジナルファイルを暗号化してブラインドファイルを作る

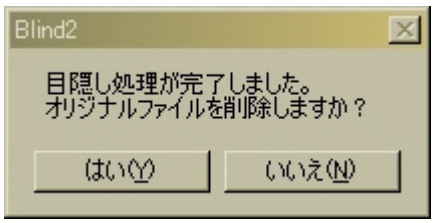


A) Blind2を起動します。

B) 暗号化したいと思うファイル（オリジナルファイル）をエクスプローラなどから「ブラインド窓」へドラック・アンド・ドロップでBlind2へ登録します。登録した結果は暗号化の対象となるファイルとして「暗号化／復号化ファイル名の表示枠」へパス名が表示されます。
ファイルではなくフォルダをドラッグ・アンド・ドロップした場合はフォルダは暗号化の対象ではありません（暗号化できません）のでその旨が表示されエラーとなります。

C) 次にパスワードを指定します。「パスワードを使用」にチェックがあることを確認、もしくはチェックを付けるとパスワード入力欄に文字列の入力が可能になります。パスワードは1文字以上、16文字以内の英数字を半角文字で入力します。英字の大文字・小文字を厳密に区別します。 大文字の A と小文字の a はまったくの別物です。また、記号や全角文字はパスワードとして使えませなので注意してください。もしパスワードに指定の文字種以外の文字があった場合はメッセージにその旨が表示されエラーとなります。
入力したパスワードが伏字（＊）になるかそのまま表示されるかは設定画面での設定によります。

D) これで「暗号化／復号化 開始」ボタンをクリックすれば暗号化が始まります。指定したファイルのサイズによっては長時間かかる場合がありまが、クリックしたボタンのすぐ下に完了したパーセント値が表示されます。また完了するとチャイム（サウンド）で知らせるようになっています。さらに設定画面で「変換後 元のファイル」を削除するか否かで「問い合わせる」に設定されていたら完了した時点で以下の画面（ダイアログ）か表示されます。



画面の中の「目隠し処理」とは暗号化のことです。ここで「はい」をクリックするとオリジナルファイルは削除されます。「いいえ」をクリックすると削除されずに残ります。必要に応じて使い分けてくださ

い。迷ったならば「いいえ」が無難です。

E) 暗号化されたファイル（ブラインドファイル）がどこに作られるかは設定画面の設定によります。「変換元と同一フォルダ」としているのでしたらオリジナルファイルのあるフォルダに拡張子「bl2」のファイルができているはずです。これがブラインドファイルです。
例えば、オリジナルファイルが abcd.txt としたとき、ブラインドファイルは abcd-txt.bl2 という名前になります。見てのとおりブラインドファイル名からはオリジナルのファイル名と拡張子名が判断できます。

F) 先ほどの操作の中で「パスワード使用」のチェックをはずした場合はパスワード入力欄への文字列の入力ができなくなります。また入力されている場合は空白になります（削除されます）。この状態で「暗号化／復号化 開始」ボタンをクリックするとパスワードなしでの暗号化が開始されます。
このとき出来るブラインドファイル名は、先ほどの例で説明すると abcd_txt.bl2 となります。違いがわかりますか。オリジナルファイルの拡張子 txt の前の記号がパスワードを使用して作成したブラインドファイルは -（ハイフォン／マイナス記号）であるのに対してパスワードを使用しないで作成したブラインドファイルは _（下線記号）になります。
ブラインドファイル名を見ただけでオリジナルファイルのファイル名だけでなく、出来たブラインドファイルがパスワードを使用したか否かが判別できるようになっています。
オリジナルファイルの拡張子の前に _（下線記号）がついているブラインドファイルは複合化するとき、パスワードの使用なしで可能です。

2. ブラインドファイルを復号化してオリジナルファイルを復元する

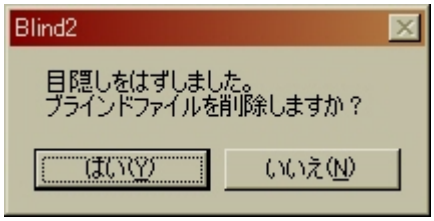
A) Bllind2を起動します。

B) 復号化するブラインドファイルをエクスプローラなどから「ブラインド窓」へドラック・アンド・ドロップします。対象となるファイルとして「暗号化／復号化ファイル名の表示枠」へパス名が表示されればOKです。
ブラインドファイルの拡張子は「bl2」です。拡張子「bl2」のファイルが「ブラインド窓」へドラック・アンド・ドロップされるとBlind2は復号化の動作をし、それ以外の拡張子の場合は暗号化の動作をします。

C) 次にパスワードを指定しますが、対象となるブラインドファイルが作成されるときにパスワードなしで暗号化されたのであれば、同じように「パスワードを使用」チェックをはずします。そうでなければ「パスワードを使用」にチェックを入れて暗号化したときと同じパスワードを記述欄に打ち込みます。半角の英数字ですが大文字・小文字を厳密に区別します。正確に入れてください。入力したパスワードが伏字（＊）になるかそのまま表示されるかは暗号化と同様に設定画面での設定によります。

D) これで「暗号化／復号化 開始」ボタンをクリックすれば復号化が始まります。指定したファイルのサイズによっては長時間かかる場合がありまが、クリックしたボタンのすぐ下に完了したパーセント値が表示されます。また完了するとチャイム（サウンド）で知らせるようになっています。さらに設定画面で「変換後 元のファイル」を削除するか否かで「問い合わせる」に設定されていたら完了した

時点で以下の画面（ダイアログ）か表示されます。



画面の中の「目隠しをはずしました」の意味は復号化をおこないオリジナルファイルを復元しましたの意味です。ブラインドファイルを残すかどうかを判断して「はい」もしくは「いいえ」のいずれかをクリックして処理が終了します。

E) オリジナルファイルが作られる場所は暗号化のときと同様に設定画面の設定によって決まります。「変換先フォルダの指定」で「変換元と同一フォルダ」としているのでしたらブラインドファイルがある（あった）フォルダに復元できているはずです。ここで注意することがあります。暗号化するときにオリジナルファイルを削除せずに残しておいた場合、その同一フォルダに復号化を試みるとオリジナルファイルと同一ファイル名となります。Blind2はこのとき上書きせずに、「オリジナルファイルが存在します」と「復号化ができなかった」という旨のメッセージを出して、エラーとしています。上書きで既存のオリジナルファイルは壊わさないようにしています。この趣旨は暗号化のときも同様で、既存のブラインドファイルには上書きはしないようにしています。どちらも既存のものが優先です。

「簡単キー」について

ブラインドファイルを作るときの厄介な問題の1つにパスワードを指定しなければならない事があります。使う側としてはパスワードは短くて覚えやすいものがいいのですが、他人が連想しそうなものであってはならず、だからといってでたらめの文字列では覚えておけない。その都度メモ用紙に書いたものを入力するのは面倒だし、かつ間違いやすい。暗号化のときにパスワードを誤入力したことをその場では気づかず、オリジナルファイルも消してしまうと．．．ブラインドファイルが残っていても大変なことになります。このことをなんとか打開しようとしたのが「簡単キー」です。

「簡単キー」とはいってみればパスワードを記録したブラインドファイル（簡単キーファイルといいます）をフロッピーディスクに書き込んだものです。暗号化することにより他人の目から隠匿します。それをフロッピーに書き込むことによりパソコンから自由に切り離し可能になり、これにより本人以外はそのパスワードを使えなくしています。ただしフロッピーの紛失には注意が必要です。

1枚のフロッピーに記録できるパスワードは1つですが、フロッピーを複数用意することにより用途により複数のパスワードを使い分けることが出来ます。また、パスワードを知っている本人は同じパスワードのフロッピーを何枚でも作れます（パスワードを知っている本人は合鍵が作れる）。これにより仲間内でパスワードを共有することもできます。しかもその仲間内には必ずしもパスワードを明かす必要がありません。フロッピーである「簡単キー」をただ預ければよいのですから。

なお、「簡単キー」のファイル（簡単キーファイル）だけを単純に他のフロッピーにコピーしても使えないようにしています。パスワードを知らない第3者は簡単には合鍵は作れないようになっています。 ・・・ただしこれは絶対ではありません。やはりフロッピーの保管は厳重にしてください。

「簡単キー」を使用する場合は「簡単キーファイル」が収められたフロッピーをパソコンにセットします。Blind2はこのフロッピーのパスワードを読みにいきます。

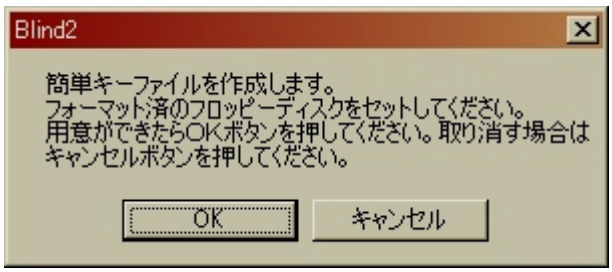
1. 「簡単キー」の作り方
「簡単キー」はフロッピーディスクに作ります。事前にフォーマット済みのフロッピーを1枚用意しておきます。

A) Blind2を起動します。

B) 「パスワードを使用」にチェックがなければ入れます。

C) パスワードを入力します。これがフロッピに書き込むパスワードになります。すなわち「簡単キー」の本体になります。ここは重要ですから、もしこのときパスワードが「伏字」の状態でしたら設定画面でパスワードを「表示する」の設定にしたほうがよいと思います。もし周りに人がいたら少しの間遠慮してもらってください。とにかく間違いのないように入力してください。
パスワードとして使用できる文字は「暗号化／復号化」の操作のときと同じですが、文字数を4文字以上としています。4文字以上16文字以内です。

D) メニューバーの「ファイル」－「簡単キー作成」をクリックします。以下のようなメッセージが出ます。指示にしたがいフロッピーをパソコンにセットして、「OK」ボタンをクリックしてください。



E) フロッピーへの書込みが始まり、書込み終了で「チャイム」が鳴ります。もしフロッピーにすでに別の「簡単キー」ファイルがあったらその旨と「上書きしますか」メッセージが出ます。「OK」もしくは「キャンセル」で「上書き」か「処理中断」を選択できます。

F) 「簡単キー」がフロッピーに作成されると同時にそれを使う準備もなされます。「簡単キー」を使う準備が出来たことは通常は「ブラインド窓」の下に鍵マークが表示されることで確認できます。また、タイトルバーは「 Blind2 － ［簡単キー］BKY無期限 」の表示になります。これらの表示がなされているとき「簡単キー」を使用して「暗号化／復号化」を行うことが出来ます。

G) 「簡単キー」が作られるとフロッピーの中には kantan. bky というファイルが1個出来ているはずです。エクスプローラで確認できます。これが「簡単キー」の本体です。
今後このkantan. bkyのことを「簡単キーファイル」と称しています。正確には「簡単キー」とは簡単キーファイルを適正に格納したフロッピーディスクのことです。
簡単キーファイルを別のフロッピーにコピーしてもBlind2はこのフロッピーを「簡単キー」と認めません。したがってバックアップ等は無駄です。合鍵を作るには基本的には先ほどの操作を繰り返すしかありません。パスワードの入力のときは、クリップボードを利用した「コピー」と「貼り付け」を使って誤入力を避けるようにしてください。
作業が終わったなら関係ない文字列をダミーでコピーしてクリップボードの中を消すことを忘れないようにしてください。一旦パソコンを終了させるのもいい手です。それでクリップボードの内容は消えます。

2. 「簡単キー」の使い方
「簡単キー」の使い方ををBlind2を起動したところから説明します。

A) Blind2を起動します。

B) 「簡単キー」のフロッピーをパソコンにセットします。「簡単キー」が手元にない場合は「簡単キーの作り方を参照して、あらかじめ作っておいてください。

C) 「簡単キー読込」ボタンをクリックします。フロッピーへのアクセスが始まり簡単キーファイルを読み込みます。

D) 読み込みが終了すると「ブラインド窓」の下に鍵マークが現れます。この鍵マークが表示されると「簡単キー」を使う準備が出来た証です。準備が出来たならフロッピーを抜いてください。実際に「簡単キー」を使って暗号化／復号化の処理をおこなうごどにフロッピーを参照するわけではありません。Blind2で読み込んでしまえばフロッピーは抜いてかまいません。

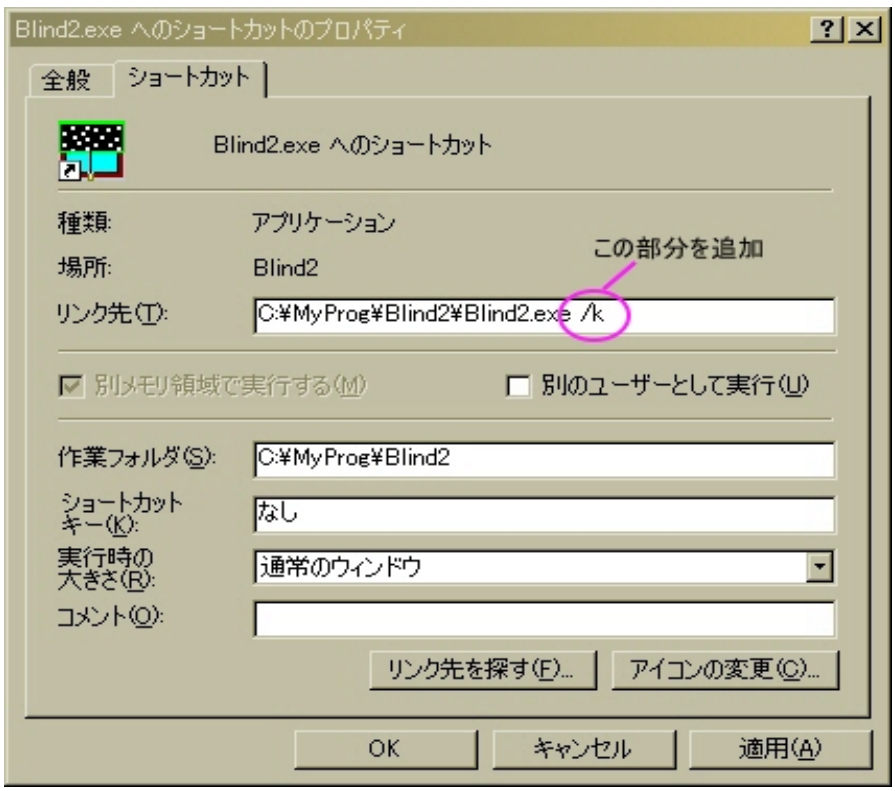
E) 「簡単キー」に仕込まれたパスワードでファイルの暗号化／復号化を行う場合は「パスワードを使用」のチェックをはずした状態で行います。
あとは通常の暗号化／復号化の手順と同じように「ブラインド窓」に対象となるファイルをドラック・アンド・ドロップして「暗号化／復号化 開始」ボタンをクリックするだけです。
同様の状態でもし「簡単キー」を読み込んでいない（鍵マークが表示されていない）とき行うと「パ

スワードなし」で暗号化／復号化がなされます。これが鍵マークが表示されているときは「パスワードなし」ではなく、代わりに「簡単キー」に仕込まれたパスワードが使われるということです。

F) 鍵マークが表示されている状態でも「パスワードを使用」にチェックをいれると通常の手入力によるパスワード指定が出来ます。その後再び「簡単キー」による作業をする場合は「パスワードを使用」のチェックをはずします。

G) 鍵マークが表示されている状態で「パスワードなし」で暗号化／復号化を行いたい場合は、現在読み込んでいる「簡単キー」をクリア（読み込んでいない状態に）する必要があります。
簡単キーをクリアするには、表示されている鍵マークをダブル・クリックしてください。これで鍵マークが消え、「簡単キー」を読み込んでいない状態に戻ります。後は「パスワードを使用」のチェックをはずせば通常の操作で行えます。
再度「簡単キー」を使う場合はあらためて「簡単キー」を読み込む必要がありますが簡単キーファイルは非常に小さいのでこのための手間隙は感じないと思います。

H) 起動オプションに半角で /k を指定するとBlind2の起動時に「簡単キー」を自動的に読込みませることができます。
具体的にはBlind2の実行ファイル（Blind2.exe）のショートカットをデスクトップなどに作成し、そのプロパティを開きます。リンク先のBlind2.exeの後ろに半角スペースを一文字置いて /k と打ち込みます。あとは修正したショートカットをクリックすればBlind2の起動と同時にフロッピーを読みに行きます。「簡単キー」フロッピーがセットされていれば読み込んだ状態で起動されます。



リンク先、作業フォルダはインストールの環境によって異なります。画像の表示と違っていても変更の必要はありません。

I) 複数の「簡単キー」を持っていてフロッピーを取り替えながら作業をする場合は注意してください。Blind2が使用する「簡単キー」のパスワードは差し込んであるフロッピーの「簡単キー」のではなくて、読み込んでいる「簡単キー」のものを使います。差し込んだだけでは使える状態にはならないことを充分念頭においてください。
また、「簡単キー」の読込きのとき、すでに読込ませている「簡単キー」をその都度クリアする必要はありません。鍵マークがついている状態で上書き読込みでかまいません。
複数の「簡単キー」を使っている場合、現在どの「簡単キー」を読込ませているかの表示が画面からは判りませんのでこの点は注意してください。

J) 「簡単キー」に仕込まれているパスワードを確認することが出来ます。この機能は「簡単キー」を作成したパソコン(オーナーパソコン)でのみ可能です。
「簡単キー」のオーナーパソコンで「簡単キー」を読込み、以下の操作を行います。

1. 「パスワードを使用に」チェックを入れます。
2. キーボードの「Shift」と「Ctrl」と「Alt」の3つのキーを押した状態で、鍵マークをクリックします。
3. パスワードの入力欄に「簡単キー」に仕込まれたパスワードが表示されます。パスワードが伏字になる場合は設定画面で「パスワード表示」を「表示する」にしてください。

使用条件

このプログラムはフリーソフトです。配布は自由です。ただし配布は blind2_nnn.lzh(nnn はバージョンナンバー)のアーカイブ単位で行ってください。プログラム単独での配布はご遠慮ください。
また作成者は著作権を放棄していません。著作権は作成者である「天本宣雄」にあります。
このプログラムを動作させ使用することにより被害を被った場合の保証等は一切行いません。その義務もないとします。
このプログラムは個人が手軽に使うことを前提に作りました。気軽に、しかも簡単に、暗号化と復号化ができればよいという主旨でつくっています。データの安全性についてはある程度考慮しましたが、個人データを覆い隠す「ブラインド」であっても、頑丈な「金庫」ではありません。使う場合はその旨を心得てお使いください。

ご意見、ご要望、バグ報告などありましたら下記までお願いします。
天本宣雄 電子メール nobuo.amamoto@nifty.ne.jp